WHAT IS CLAIMED IS:

1. A method of decrypting contents information, comprising the steps of:

generating a signal representative of a key in response to key production information, the key being for decrypting encryption-resultant contents information;

decrypting the encryption-resultant contents information in response to the generated signal representative of the key;

receiving key-related information which has been generated by an external in response to an authentication value and at least a portion of the key production information according to a predetermined function;

receiving issue ID information which has been generated in response to the authentication value and decryption-side ID information peculiar to a decryption side;

reproducing the authentication value from the decryption-side ID information and the received issue ID information; and

generating at least a portion of the key production information from the reproduced authentication value and the received key-related information according to a function inverse with respect to the predetermined function.

2. A method of decrypting encryption-resultant contents information generated by an encryption side which implements the steps of generating a first-key signal representative of a first key

from first-key base information being a base of the first key; encrypting contents information into encryption-resultant contents information in response to the first-key signal; generating a second-key signal representative of a second key from second-key base information being a base of the second key; encrypting at least a portion of the first-key base information to convert the first-key base information into encryption-resultant first-key base information in response to the second-key signal; and generating second-key-related information from the second-key base information and an authentication value according to a predetermined function; the method comprising the steps of:

receiving issue ID information which has been generated in response to the authentication value and decryption-side ID information peculiar to a decryption side;

reproducing the authentication value from the decryption-side ID information and the received issue ID information;

reproducing second-key base information from second-key-related information and the reproduced authentication value according to a function inverse with respect to the predetermined function;

generating a second-key signal representative of a second key from the reproduced second-key base information;

decrypting encryption-resultant first-key base information into original first-key base information in response to the generated second-key signal;

generating a first-key signal representative of a first key from

the original first-key base information; and

decrypting encryption-resultant contents information into original contents information in response to the generated first-key signal.

3. An apparatus for decrypting contents information, comprising:

means for generating a signal representative of a key in response to key production information, the key being for decrypting encryption-resultant contents information;

means for decrypting the encryption-resultant contents information in response to the generated signal representative of the key;

means for receiving key-related information which has been generated by an external in response to an authentication value and at least a portion of the key production information according to a predetermined function;

means for receiving issue ID information which has been generated in response to the authentication value and decryption-side ID information peculiar to a decryption side;

means for reproducing the authentication value from the decryption-side ID information and the received issue ID information; and

means for generating at least a portion of the key production information from the reproduced authentication value and the received key-related information according to a function inverse with respect to the predetermined function.

4. An apparatus for decrypting encryption-resultant contents information generated by an encryption side which implements the steps of generating a first-key signal representative of a first key from first-key base information being a base of the first key; encrypting contents information into encryption-resultant contents information in response to the first-key signal; generating a second-key signal representative of a second key from second-key base information being a base of the second key; encrypting at least a portion of the first-key base information to convert the first-key base information into encryption-resultant first-key base information in response to the second-key signal; and generating second-key-related information from the second-key base information and an authentication value according to a predetermined function; the apparatus comprising:

means for receiving issue ID information which has been generated in response to the authentication value and decryption-side ID information peculiar to a decryption side;

means for reproducing the authentication value from the decryption-side ID information and the received issue ID information;

means for reproducing second-key base information from second-key-related information and the reproduced authentication value according to a function inverse with respect to the predetermined function;

means for generating a second-key signal representative of a

second key from the reproduced second-key base information;

means for decrypting encryption-resultant first-key base information into original first-key base information in response to the generated second-key signal;

means for generating a first-key signal representative of a first key from the original first-key base information; and

means for decrypting encryption-resultant contents information into original contents information in response to the generated first-key signal.

5. An apparatus as recited in claim 3, wherein the issue-ID-information receiving means comprises an input device for enabling a user to input the issue ID information.

6. A method as recited in claim 1, wherein the issue-ID-information receiving step comprises receiving the issue ID information after it has been confirmed by a sender for the issue ID information that the decryption-side ID information is legitimate.

Add A1